

DOCUMENT RESUME

ED 282 789

SO 017 839

AUTHOR Wildavsky, Aaron
TITLE The Secret of Safety Lies in Danger.
PUB DATE Dec 85
NOTE 35p.; Paper presented at the Conference on the Bicentennial of the U.S. Constitution (Provo, UT, January 16-17, 1986).
PUB TYPE Reports - Descriptive (141) -- Speeches/Conference Papers (150)
EDRS PRICE MF01/PC02 Plus Postage.
DESCRIPTORS *Accident Prevention; *Appropriate Technology; Human Resources; Innovation; Opportunities; *Prevention; Public Policy; *Risk; *Safety; Technological Advancement

ABSTRACT

In creating and maintaining public safety, risks which entail some amount of danger are necessary. These risks must be rated regarding the amount of benefit and danger they would bring in order to ascertain the worthiness of the risk. It is important to realize that risks can often bring greater safety, that many safety devices themselves involve risk, and that focusing negatively on risks creates a bias towards technological inaction, which is very dangerous. Trial and error risk-taking proves better than risk aversion in securing safety, because it helps build resilience to dangers, a resilience that makes necessary risks less potent. Moreover, safety and danger are interwoven into the same objects and practices. (AEM)

* Reproductions supplied by EDRS are the best that can be made *
* from the original document. *

December 1985

THE SECRET OF SAFETY LIES IN DANGER

Aaron Wildavsky

Political Science Department,
Graduate School of Public Policy,
and
Survey Research Center

University of California, Berkeley

Prepared for a Conference on the Bicentennial of the U.S.
Constitution, "The Constitution, Government Regulation and
Public Policy," Brigham Young University, January 16-17, 1986

U.S. DEPARTMENT OF EDUCATION
Office of Educational Research and Improvement
EDUCATIONAL RESOURCES INFORMATION
CENTER (ERIC)

✓ This document has been reproduced as
received from the person or organization
originating it.
☐ Minor changes have been made to improve
reproduction quality.

• Points of view or opinions stated in this docu-
ment do not necessarily represent official
OERI position or policy.

"PERMISSION TO REPRODUCE THIS
MATERIAL HAS BEEN GRANTED BY

Aaron
Wildavsky

TO THE EDUCATIONAL RESOURCES
INFORMATION CENTER (ERIC)."

Of the many new things in the Constitution of the United States, perhaps the most important is not directly stated: the belief that mankind might design rather than inherit or have imposed upon them the institutions under which they govern themselves. Self-government is a noble, indeed one might well say a risky enterprise. How were the risks apportioned?

Without free institutions dependent upon public support there could be no self-government. Yet the very existence of central institutions empowered to exert coercive authority over individuals, the crucial difference between the Articles of Confederation and the Constitution, opened up the possibility of abuse. How, then, rate the risks?

Every institutional actor is considered risky, i.e., prone to abuse. That is why powers are separated. Powers are not merely shared to prevent abuse, they are also dispersed to encourage innovation in the form of a multiple approach to problems. The framers felt able to anticipate a few major problems, such as war and debasement of currency. For these they created as strong a central authority as consent of the governed would permit. For the rest, expecting that life would reveal difficulties of which they and their successors might well remain unaware, they dispersed the capacity to consider the unknown

as widely as possible. The residual police power to secure the general welfare was left with the states. The glittering generalities for which the Constitution is famous constitute a rejection of the view that central authority knows best. In that case a long list of dangers to be avoided would be followed by an even longer list of policy prescriptions for avoiding them. Instead, a House of Representatives based on population, a Senate elected by state legislatures, and a president presumably chosen by local elites with national reputations, are placed in partly cooperative and partly conflicting relationships and then superimposed upon a federal structure so that diverse views of dangers--geographical, social, philosophical--are considered.

The framers placed the resilience of the system ahead of the safety of its parts. It was in the system as a whole rather than the sanctity of its parts that such safety as is given to human beings was thought to reside. The paper that follows seeks to build strategies for securing safety from technology on the foundations of similar principles.

THE SECRET OF SAFETY LIES IN DANGER

Contrary to current doctrine, "trial and error" is safer than "trial without error." Opportunity risks are exceeded by opportunity benefits. Highly dangerous, low probability events are overwhelmed in importance by highly probable, low benefit actions. Richer is safer, not sicker. Resilience is superior to anticipation as a strategy for reducing risk. Playing it safe hurts people. Adding to the pool of global (flexible, fungible) resources secures safety for more people than trying to protect any single part of the population against adversity. Since safety has to be discovered, not merely chosen, trial and error risk taking (unless strong evidence exists to the contrary) rather than risk aversion is the preferred strategy for securing safety.

Global Resources

Safety is a function of the general, global level of resources in a given society at a certain time. By general resources I mean knowledge, education, wealth, and any other resource (energy is a proxy for national product) that can be used for diverse purposes. General resources, like the primary colors, are fungible: they can be converted into other things. They are not just food crops but the

capacity to grow food and to alter what one grows according to the conditions of the time. The global level stands for overall resource capacity--the ability to convert and to redeploy resources.

Conceivably, there could be a limit on global resources, a limit not only at an instant in time but for all time thereafter. While the materials out of which energy is transformed should last for eons, for instance, it is possible that at some time their cost will increase. Where physical resources may be limited in amount and usability (a topic covered under the elusive subject of entropy), however, the currency of human ingenuity is information and I am not aware that it faces exhaustion.

Improvement in overall capability, i.e., a generalized capacity to investigate, to learn, and to act, without knowing in advance what one will be called to act upon, is a vital protection against unexpected hazards. Acquired Immune Deficiency Syndrome (AIDS) is a recent example. An editorial in Nature observes that

. . . the understanding of AIDS that has now been wrung from a seemingly obdurate problem is striking proof of the value of the basic biomedical research on which people have for decades enthusiastically lavished their talents--and governments, less sure of themselves, their resources.

In these terms, rapid demonstration that AIDS is indeed caused by a virus is a triumph The triumph is that the research community has been able to respond so quickly to an unexpected development such as the emergence of AIDS. The explanation is again simple, exasperatingly so--the richness and diversity of the biomedical research enterprise in the United States in particular but also throughout the world.*

The Axiom of Connectedness

Dangers will arise; everyone agrees on that. Uncertainty about the consequences of present acts and about others as yet unforeseen cannot be reduced to zero. The axiom of ever-present uncertainty is based not only on the self-evident premise that no one knows it all but on the slightly less obvious consideration that as human beings act on their environment they create still more consequences of which they are as yet not fully aware. Although some uncertainties may be reduced under some circumstances, a modicum of uncertainty is a universal condition. Hence Kenneth Boulding writes about "irreducible uncertainties." **

*Science, Vol. 309 (May 3, 1984), pp. 1-2.

**Kenneth Boulding, "Irreducible Uncertainties," Society, Vol. 20, no. 1 (Nov./Dec. 1982), pp. 15-17.

To the axiom of ever-present uncertainty I wish to add another: The axiom of connectedness states that the good and the bad (safety and health effects) are intertwined in the same acts and objects. There may be unalloyed goods (though I doubt it; after all, even a perfect safety record may tempt us to lower our guard) but, if so, they are few and far between. Taking the two axioms together--uncertainty cannot be eliminated and risk cannot be avoided--stipulates the conditions under which the question of how to increase safety should be considered.

Suppose the things of this world, the substances in it and the practices people follow, were all good or all bad for securing safety. Then nothing (including differences between local and global effects) would matter, except the injunction to discover and choose the good and discard the bad. The end--secure safety--is given and a decision rule is known for choosing among available means. But life is not so simple or straightforward. For the most part, safety and danger are interwoven into the same objects and practices. Under the right (or wrong) conditions, everything we need for life can maim or kill: water drowns, food poisons, air chokes. Since there are many, many things out there, interacting in innumerable ways, moreover, the axiom of connectedness--the good and the bad are mixed in the same objects--must be generalized to the relationships among them. Everyone is likely to do something or be subject to some elements not good for them. The trick is to get more of the better and less of the worse.

Safety is a Balancing Act

Without trial there can be no new error, but without new error there is also less new learning. Science, its historians say, is more about rejecting than accepting hypotheses. Knowledge grows by criticizing the failure of existing theory to explain or predict events in its domain of applicability. Learning by criticizing implies that existing theory is in error, not necessarily absolutely, but relative to better, though never perfect, knowledge. Rules for democracy say little about what one does in office, but much more about getting officials out of office. "Throwing the rascals out," is the essence of democracy. Similarly, in social life, it is not the ability to avoid error entirely (even Goncharov's Oblomov, who spends his life in bed, cannot do that), but learning how to overcome it that is precious.

Even if it were true that following the principle of trial and error would provide for more health than harm, it is possible that people would still be better off by not allowing certain things to be done. Why not, then, follow public policy in the United States by prohibiting new things unless they are proven to be safe? Indeed, why take chances with public health? The assumptions required to make good this proposition--no trials without prior guarantees against error--are hard to meet. The first such assumption is that the safety benefits of trial and error would be maintained while only its harms would be

eliminated. While the desire to pick the eyes out of the potato of life is understandable, it is not achievable. For a second assumption requires that society, acting through government, know the difference between actions that will increase or decrease safety in advance, allowing the good to go on and stopping the bad. Otherwise, harm will be done to more people by preventing actions that would have made their lives somewhat safer.

The most persuasive and the most common argument against learning by trial and error is that it should not be used unless the consequences of worst case errors are sufficiently benign to permit new trials. If errors lead to irreversible damage to large populations, there may be no one around to take on the next trial.

Playing It Safe Is Dangerous

The most seductive form of playing it safe is prudential conservatism: when in doubt, add margins of safety. Why be half safe? Why allow anything new unless it can be shown to do no harm? Better not to ceaselessly search for novelty

but rather to insist that the new do good. In such fields as toxicology and engineering, conservatism has honorable precedents.

But how much conservatism should there be? First, one estimates the dangers of a product or practice according to existing knowledge. At every step there are decisions to be made as to where to bound uncertainties. Caution, presumably, is the byword. Having arrived at an estimate (or range of estimates), one chooses the upper bound of danger. Then that upper bound is multiplied by a safety factor of, say, ten to a hundred. Observe what has occurred. As uncertainties are repeatedly resolved by exaggeration, then multiplied by others similarly manipulated, estimates of potential damage may be increased thousands of times over. So what? What is wrong with being super-cautious?

There is no stopping point. If super-caution is to be the guiding principle, there is no reason why estimates should not again be increased so as to become even safer. Since virtually everything has some harm in it, extending that degree of danger by conservative calculation is bound to show that the activity in question should be disallowed.

In order to comprehend the consequence of rejecting trial and error by counting only costs, without allowing compensating benefits, an example from everyday life is in order. Were no errors permitted, no hospital in the world

could stay open. Since people get sick from being in hospitals, a phenomenon called iatrogenic (hospital-related) disease, these organizations would have to be closed, despite the good they do,* on the undeniable ground that they also do harm. The same is true for vaccines. By penalizing the small damage done, without offsetting it with the big benefits, society is endangered.

Trial Without Error as Public Policy

The doctrine I have been discussing--no trial without prior guarantees against error--is embodied in practice. Old products and substances are still subject to trial and error in that the burden of proof justifying regulation is on government, but new ones operate under the rule of "no trials without prior guarantees against error" in which producers have the affirmative obligation of proving that their product will do no harm.**

The disinclination to consider benefits while focusing largely on costs creates a bias towards technological inaction. Yet there are reasons for society to encourage trial and error risk-taking. By reducing old, still-existing dangers, not merely avoiding new ones, risk taking is made

*

**Peter Huber, "Exorcists vs. Gatekeepers in Risk Regulation," Regulation (Nov./Dec. 1983), pp. 23-

socially desirable. There are not merely new gains or losses but old hazards to be eliminated or alleviated in ways that improve human life. I call these "opportunity benefits." The opportunity cost of a given expenditure, following the concept used by economists, is the other valued goods that might have been purchased with the same resources. The opportunity risk of a given act or policy, as defined here, is the additional danger brought about by doing or producing something new. This general concept, if not the particular dangers, is well understood in common parlance about risk. Hardly understood at all, perhaps because not yet formulated, is the concept of opportunity benefit--the loss of opportunity to reduce existing harm that society foregoes as a consequence of decisions to delay or deny the introduction of a new substance or technology. Wise decision making should consider not only the opportunity risks but the opportunity benefits, the chance to diminish existing dangers, inherent in a given act.

An advantage of trial and error is that it renders visible hitherto unforeseen errors. Because it is a discovery process that makes latent errors manifest, so we can learn how to deal with them, trial and error reduces the scope of unforeseen dangers and hence lowers risks.

Rosenberg argues that "many significant characteristics of . . . products are revealed only after intensive or, more significantly, prolonged use."* Technological innovation is mostly accomplished by users who modify, not designers who originate, products. The potential of a product depends not only on what is in it but also on how others choose to use it. And what these relevant others do depends on what they learn both about the thing itself and the uses to which it might be put. Users are more numerous and more diverse than producers. Their number and diversity suggest that more tests in use will be made under more varied conditions. The larger the number and the greater the variety of hypotheses tested ("Is this produce satisfactory under my conditions?"), the greater the probability of learning about good and bad impacts and the conditions under which they apply. No trials, no users, no learning, no mitigation of existing dangers.

Both doing something and doing nothing can be dangerous. Acts of omission--failing to take advantage of opportunity benefits--as well as acts of commission--damage to health by trying something new--can lead to making life less safe. Whether and to what extent action or inaction is safer must depend on the balance of circumstances. As political

*Nathan Rosenberg, "Learning by Using," Chapter 6, Inside the Black Box: Technology and Economics (Cambridge Univ. Press, 1982), pp. 121-40.

radicals are wont to say in reaction to conservatives, inaction is action in support of the status quo. Yet the existing state of affairs contains hidden harms that might well be mitigated were society to secure opportunity benefits.

The iron law of skiing--you are not learning unless you are falling--exemplifies learning from mistakes while suggesting a condition limiting this process: errors must not be made on purpose. If all you do is fall down, you will not be able to distinguish between better and worse technique. You have to be making an effort to be error free (while realizing you won't succeed) in order for error to tell you what you don't know. You even have to succeed to some extent in order to differentiate error from something better. Thus real progress arises from mistakes that occur when you are doing everything you know how to avoid error. Both trying to avoid error and still experiencing it are essential. And these are essential attributes of market processes.

Markets and Safety

Does economic competition increase safety? Why, given the desire for individual advantage in economic markets, does society end up benefiting by better health? For everywhere in the world, within and among nations and groups, the richer are indeed healthier. Economists, so far as I know, have not turned their attention to the relationship between markets and safety.

If income and health are positively related, it stands to reason that the larger the proportion of the population with higher incomes, the better the health of the nation's people on average. And since we know that being surrounded by educated people improves the safety of the entire area, there may be positive contagion effects: the healthier one's neighbors, the healthier one is likely to be.

This is the postulated line of causality: competition increases income which provides protection for people's health. The direct effects come from public health and medicine. The indirect effects, which are much larger, operate through material advantages, such as food, educational benefits, such as superior safety practices, and technological progress, which teaches us how to do things better, including how to have our cake--higher incomes--and eat it too--while improving our health.

Rather than attempting to anticipate hazards before they occur, unless the risks are compelling, market processes work to increase wealth so as to be able to respond resiliently to dangers as they manifest themselves. In addition to creating wealth, markets also combine decentralized anticipation (numerous independent probes of an uncertain future) with pluralistic resilience (learning how to cope with danger by diverse groups) so as to achieve a greater degree of safety. The ability of market competition to interrogate the unknown at a low cost to society, while simultaneously encouraging individuals to overcome adversity, has been under-appreciated. Another way to pose the question that has occupied us is to ask whether and in what respects and under which conditions strategies of anticipation are better or worse than strategies based on resilience?

Anticipation versus Resilience

Anticipation is a mode of control by central cognition; efforts are made to predict and prevent potential dangers before damage is done. Resilience is the capacity to use change so as to cope better with the unexpected. It is learning to bounce back. Are risks better balanced, we may ask, by attempting to anticipate them before they occur or by trying to mitigate their effects after they have manifested themselves? What proportion of anticipation and of resilience is desirable under which conditions?

Resilience is concerned with realized hazards; anticipation attempts to avoid hypothesized hazards. If it were possible (1) to anticipate efficiently, that is, to predict (or guess) right often enough to make up for the costs of guessing wrong, and (2) to react effectively--controlling the expected condition so as to leave life better off--anticipation would be the preferred strategy. Why suffer unnecessary damage? Usually, however, the uncertainties are so substantial that we cannot tell in advance which ones among a multitude of hypothesized dangers, if any, will actually turn out to be the real ones. Consequently, the effort to anticipate all or most dangers is likely to lead to a societal immune reaction: death not through invasion but through exhaustion as resources are used up in a futile effort to anticipate the future.

A strategy of resilience does not mean waiting for a disease to strike before trying to respond to it. Rather, it means preparing for the inevitable, the appearance of a new disease, by expanding general knowledge, technical facility, and command over resources. If this knowledge were to be sought in an effort to anticipate particular diseases, it would be less useful than if it could be directed at a broader range of dangers.

The rationale for reliance on resilience as the major strategy lies in inherent uncertainty; if, try as we may, we are not likely to be successful anticipators, we resort to resilience. For resilience is an inferior strategy only when rather strict conditions--know what, know when, know how, know how much, act as indicated--are met. Resilience is a superior strategy for making use of inherent uncertainty to do better. The evidence from ecological studies is suggestive: anticipation suits organisms that flourish in a narrow niche; resilient organisms that learn how to cope with adversity do much less well in any single niche but better over a number of environmental bands.

Going to extremes--all resilience, no anticipation, or vice versa--would be destructive. If you have no protection against expected and controllable hazards, you would constantly be faced with foreseeable emergencies that will be dealt with too late, too hastily, and too wastefully. Were there dangers with irreversible consequences, we would be overwhelmed before we could act. Followed faithfully, a strategy of anticipation might well use up all resources in a vain effort to guard against unknown (and, perhaps, unknowable) danger. What to do?

Anticipatory actions do have their place in a sensible safety strategy; the difficulty is to know what mix of anticipatory and resilient measures is optimum. Given inherent uncertainties, in my opinion, a little anticipation goes a long way. Instead of attempting to guard against most dangers, only the most likely or most dangerous should be covered, fully expecting that whatever was missed would be countered as and after it occurred, thereby building up resilience for the unknown danger that will surely come.

Interrogating the Unknown

It is useful to distinguish between certainty--the ability to predict the consequences of actions--and uncertainty--knowing the kind or class of events that will occur but not the probability of their happening. Ignorance involves knowing neither the class nor the probability of events. When we are uncertain, we know about the type of events that will occur but not how likely they are to take place. But when we are ignorant, we do not know either how likely the consequences of our actions are nor what class of consequences--hail storms, burst dams, train wrecks, economic decline--will confront us. Yet we can be still worse off. Ignorance may be exceeded by super ignorance--thinking we know and not knowing we don't know. And super ignorance itself may give way to astonishment--expecting one class of events and getting another. Surprise, as I shall use the term, is based on ignorance. Astonishment occurs when super ignorance results in anticipatory measures that lead to overconfidence.

Now there are at least two kinds of surprise. One might be called quantitative surprise. We know the kind of thing that can happen but are surprised by the fact that it occurs more frequently than we had supposed. I call this expected surprise because we know it is coming but not how often. The other category is qualitative surprise. This is "true" or unexpected surprise.* My thesis is that the growth of resilience depends upon learning how to deal with the

* Qualitative surprise might more simply be called "ignorance." But I prefer to reserve that term for situations where neither the class or the probability of consequences are known but the ignorant do not know that they don't know. A beginning taxonomy of ignorance is provided by Robert Wolfson and Thomas Carroll:

By ignorance we mean that state of knowledge wherein the decision maker lacks awareness of some objectively possible states of the world which he faces. We can detail three types of ignorance.

1. Ignorance of actions. There are some actions which are objective alternatives but about which the individual is unaware. We take this to mean that he is in ignorance of all outcomes attributable solely to these unknown alternatives.

2. Ignorance of outcomes. There exist some outcomes of which the decision maker is completely unaware. He believes that the n outcomes he has in mind

unexpected, a term that Jerome Bruner identifies as striking "one with wonder and astonishment," i.e., with qualitative surprise.*

Since it is neither possible nor desirable to anticipate all actual catastrophes, what is wanted is a method for interrogating the unknown. This method should pick out both potential trouble and potential advantage, sample each, give society some experience in warding off or coping with the bad

constitute the full set of consequences attributable to a particular set of actions; but in fact there are m others.

3. Ignorance of values. There are some outcomes of which he is aware, but whose nature is a complete mystery to him. That is there are n possible outcomes which he knows well enough to say that if the ith occurs, it will benefit or disadvantage him in some imaginable manner and/or amount. There are m others which he knows might occur, but which he cannot describe in any such fashion. (Robert J. Wolfson and Thomas M. Carroll, "Ignorance, Error, and Information in the Classic Theory of Decision," Behavioral Science, vol. 21, 1976, pp. 107-115.)

* Jerome S. Bruner, "The Conditions of Creativity," in Howard E. Gruber, et al, eds., Contemporary Approaches to Creative Thinking (Prentice Hall, 1962).

and taking advantage of the good, without requiring a huge expenditure of resources or premature commitment to a single approach. The more people that participate in this strategy, the more widespread the search, the more diverse the probes and the reactions, positive and negative, the better. Evidently, this method should be democratic--decentralized, participatory, based on diverse and repeated probes and responses by various people differently situated.

This method is familiar to us. It belongs to the family of self-organizing systems. It is a form of social spontaneity, not social control. It is called, though it is not just any kind of, trial and error.

Until now I have not asked a crucial question about the strategy of anticipation, namely, anticipation by whom? It is all too easy to assume that governments or other large collective entities must do the anticipating. That is why we are so concerned about resource depletion following upon wrong prediction. Aside from the difficulty of arriving at collective judgments about theory through bureaucratic procedures, we are concerned about conjectures turning out to be false because the implications are so large. Since preventive measures are so expensive, and their consequences so profound, the need to be right is far greater than limited knowledge of cause and effect can support.

Suppose, however, that anticipation is decentralized. There are very large numbers of anticipators (think of them as

entrepreneurs trying out new products or users modifying old ones), each of whom pays not all but a substantial part of the cost of error. Should they fail to predict future events, they bear the financial costs. Should their products turn out to harm others, they can be sued. Instead of society guessing about consequences, it can hold producers to account for the actual damage they do.

While spurring innovation, to be sure, the discovery procedure called trial and error is also creating new knowledge of actual consequences, some which will undoubtedly be bad. How, its critics ask, can anyone be given the right to impose unknown harm on others? Hence they propose the rival doctrine of allowing no trials without prior guarantees against error. Alongside these undoubted costs to society, however, opportunity benefits are being created. And one of these, not previously discussed, is exploration of the unknown. For it is precisely the lack of central control and command that permits a wide variety of hypotheses to be tested so as to vigorously sample the unknown, thus bringing us into contact with events about which we would otherwise have been ignorant and in regard to which one or another of us would not have garnered experience.

If it is experience in coping that is desired, an evident riposte goes, why not institutionalize fire drills or other exercises designed to give practice in responding to

emergencies? A strategy of expected surprise has its uses. Practice may well make perfect, though, if the expected danger is long delayed, one observes lax compliance. Emergency preparedness makes sense so long as one has the right emergency in mind. For qualitative or real surprise, however, there are no ready-made drills. The underlying premise of expected surprise is that the unknown risks must be limited to the same sorts of risks that you deliberately practice to meet through planned failure. Precisely because it fails to interrogate the unknown, a strategy of expected surprise provides only the appearance but not the reality of resilience.

The way to keep society's coping mechanisms well exercised is not through deliberately tolerating known and avoidable sorts of failure, but through progress, since only new development keeps producing unpredictable risk situations. Only managing these presently unknowable hazards keeps coping ability in shape. Even better, because such progress-related risks can be viewed as a statistical sampling from the entire universe of possible unforeseen risks, successfully coping with such risks as arise from progress does provide real information about most possible risks. Hence, our coping mechanisms will, most likely, be strengthened in just the sorts of ways that will be needed against the truly unexpected. This is another reason why a rapidly progressing society will usually be safer than a static one.

Does Adding Safety Devices Increase Safety?

Against this rather rarified wisdom--rely on resilience--may be posed the urgings of common sense: When you see an opportunity to increase safety, take it. Theorists may talk all they want about roundabout strategies of resilience but direct strategies of anticipation, the bird in hand, are preferable. A straightforward statement of this proposition would be that adding measures designed to secure safety actually increase safety. But do they? Because adding multiple safety measures has been the practice of the nuclear power industry, under the whiplash of regulation, a study of the inspection of nuclear power plants provides an opportunity to explore the direct, anticipatory hypothesis: Take safety measures to increase safety.

Nuclear welding codes require the reworking of welds in which even tiny voids occur; rework itself, however, can weaken the materials used (e.g., stainless steel pipe). Given differing skills among those who do the rework, it is not always clear that correction of minor defects will produce an increase in safety. Similarly, pipe restraints are often installed to prevent damage to nearby equipment from the whipping motion generated when and if a pipe rupture occurs. These restraints, however, may produce a binding of the system that decreases safety by introducing additional strain.

Testing can also be counterproductive. The availability of electrical power is essential to reactor safety. Control of the plant during normal operation and the ability to keep the plant safely shut down during emergencies depend on maintaining a reliable system of alternate electrical sources. Because offsite power is not sufficiently reliable, diesel generators are required to be installed to provide a backup onsite source. Because these generators themselves may fail to operate on demand, there are usually two or more at a given site. If the probability is relatively high that offsite power will fail, the ability to prevent any series of events that would lead to reactor core damage depends on reliable onsite diesel power. The reliability or unreliability of the emergency diesel generators determines the probability of a serious accident. Given their importance, it might seem reasonable to require that these diesel generators be tested regularly to ensure their operability. Testing, however, may not always be advisable, since the test itself may make the generator less dependable.

As a means of further increasing system reliability, it was at one point suggested by a company that during times when its power distribution grid was on "alert status," nuclear plant personnel should "idle start the diesel engines and run them for a short period of time" to verify their availability. The NRC staff agreed that this would probably be the simplest way to determine availability, but pointed out that idle starting diesel generators and running them unloaded "could unnecessarily hamper their performance in a real emergency."

Safety devices can themselves be a source of danger as well. Reactor coolant pumps are clearly essential safety features in any reactor; these pumps, however, require lubricating systems, and these lubricating systems are one important cause of fires within reactor containments.

Increasing protection in one area may create difficulties in others. Protecting against low probability events, for example, may interfere with more everyday threats to system stability. The seismic design requirements for nuclear plant piping, for example, have been continually increased. Even in the most seismically active areas, the probability that a sufficiently large earthquake will occur over the plant's lifetime is relatively low. The anticipated damage from such earthquakes is, however, quite high. Extra precautions therefore have seemed justified. Recently, though, questions have arisen concerning the consequences of adopting extra precautions to guard against such a remote "worst case."

Reinforcement of the piping system against earthquakes has some important negative consequences for the viability of the system as a whole. The parts have their own failure rates and these rates are highly dependent on the way in which they are maintained. Servicing the snubbers requires procedures which also increase the likelihood of failure. Even where the pipe support snubbers are successfully maintained and work properly, tightly bound systems are subject to much greater stress during normal operation than are more flexible systems.

Among the consequences of solving seismic problems by strengthening individual supports and adding more and more of them are (1) limitation of access for routine maintenance of equipment, (2) limitation of access for in-service inspection of equipment and the piping itself, and (3) creation of a relatively rigid system which may be less able to withstand stress in everyday operation.

A Taxonomy of Risk Errors

The beginnings of a "taxonomy of risk errors" can now be suggested. I propose six categories of such errors:

- 1) Ignoring opportunity benefits, i.e., overlooking those existing risks that will continue unabated by the choice to delay the introduction of new technology that could reduce them.
- 2) Ignoring the risks associated with a proposed remedy.
- 3) Ignoring large existing benefits while concentrating on small existing risks.
- 4) Ignoring the effects of economic costs on safety.
- 5) Ignoring the inevitable tradeoff between Type I and Type II errors.
- 6) Ignoring the displacement of risks onto other people as a consequence of reducing risks for some.

These categories are not mutually exclusive, and indeed all of them might be viewed as special examples of the same basic error, focusing only on one dimension of the overall risk situation.

Ignoring "Opportunity Benefits"

Among the experiments delayed by the moratorium on genetic engineering is an interesting effort to make crop plants selectively resistant to certain herbicides. Some of the newer herbicides are effective in very small doses--only a few grams per acre are needed rather than the kilograms per acre required for older herbicides--or else have much lower toxicities for animals and insects. But, being non-selective (in contrast to such herbicides as 2,4-D or 2,4,5-T), they will kill the desired crop as well. Both Calgene (a small genetic engineering company in Davis, California) and DuPont have developed genetic engineering methods for making crops selectively resistant to such herbicides, which would allow existing herbicides to be displaced with these environmentally safer ones. No consideration is given to the opportunity benefits, the health benefits delayed or denied, that result from the moratorium.*

*Science, Vol. 229 (July 5, 1985), pp. 34-35.

Ignoring Large Existing Benefits While Concentrating
on Small Existing Risks

Many times the remedy is worse than the disease. Safety precautions may lower small risks while increasing more major risks.

Two forms of smoke detectors are currently available in the U.S. One uses a tiny amount of a radioactive element to detect smoke, and is called an "ionizing unit." The other uses a photoelectric cell. Ionizing units cost as little as one-fourth as much as photoelectric units, and so are much more commonly used. Yet they emit radiation, and there is a move afoot to eliminate them as an unnecessary and unacceptable source of cancer risk. Entirely ignored in this thinking is the demand curve for smoke detectors. Quadrupling the cost of having any smoke detector, which would be the result if only the more expensive photoelectric units were available, will inevitably lead substantial numbers of people at the margin to decide to forego purchasing smoke detectors entirely. Since current estimates are that 7500 lives are lost each year that might have been saved had smoke detectors been in use, the risks associated with having no smoke detectors at all are neither insubstantial nor hypothetical. The opponents of the cheaper ionization unit are trading an

immeasurably small cancer risk for a quite significantly larger and also much more immediate risk of death and injury from fire.* Making smoke detectors more expensive lowers the buying power of consumers; hence, less wealth means less health. Low-income consumers must either do without smoke detectors, or forego other investments that might also increase safety.

Ignoring the Inevitable Tradeoff
Between Type I and Type II Errors

There is a kind of irreducible statistical uncertainty that limits how safe we can become, namely, the complementary relationship between Type I and Type II errors. A Type I error is falsely raising an alarm when in fact no hazard exists, and a Type II error is falsely ignoring a hazard that is in fact real. Both kinds of error are well exemplified in the fable of the boy who cried wolf. His first alarms, being false, were Type I errors, while the ignoring by the villagers of his final alarm--which was a valid one, since the wolf was indeed there--is a Type II error. The interesting thing about this fable is that it raises in a graphic way the profound

*Milton Copoulos, "It's Effective--But Is It Safe?", Reason (March 1985), pp. 29-30.

question of what sort of decision criteria the boy should have used in order to reduce his Type I error. His constant cries of "wolf" might well have arisen out of conscientiousness rather than mischievousness; they very possibly could have resulted from his having only limited and uncertain information as a basis for deciding whether or not a wolf was present--possibly only a tuft of hair on a bush, or a footprint, or a dropping, any of which could have come from a coyote or dog as well as from a wolf. Given this uncertainty, he might well have opted to be "prudent," reasoning that no one would be seriously hurt if his alarm turned out to be false, but that the village would be grievously injured if he failed to raise the alarm when a wolf truly was there. In this situation he might have decided to "err on the side of safety," by called out a warning every time an ambiguous bit of evidence came to his attention. As the fable illustrates, there was an unforeseen catch to this decision strategy: The inability to distinguish true alarms from false alarms became so great that all alarms came to be ignored, with the perverse outcome that a decision strategy chosen purposefully so as to reduce to a minimum the chance of missing a true hazard led instead to an increase in that very risk.

Roughly half of all chemicals tested in animals under the conservative rules of conducting and interpreting animal tests have turned out positive, i.e., have been judged to be "wolves." Hence, regulatory agencies are swamped with chemicals needing to be regulated. So much so, indeed, that there is a huge backlog of chemicals awaiting regulatory consideration. The core problem is that no one can know which among this vast backlog are the chemicals that pose a truly significant risk of cancer to humans, if any, and therefore deserve to be regulated first. Once again, as with the boy crying wolf, valid cancer "signals" are getting lost among the swarm of signals from trivial or falsely identified risks, i.e., there is a tremendous loss of discriminatory power inevitably associated with erring "on the side of safety." The result is that substantial regulatory resources are being expended to reduce risks that are already trivial, while the public's exposure to the carcinogens that matter is being prolonged.

Exactly this same principle can be seen in a case involving naval security. Deciding to "err on the side of safety," that is on the side of overclassifying documents, made it necessary to grant security clearances to so many people that it became impossible to investigate them adequately, and, especially, to do follow-up checks to see that they stayed loyal. In this way, a breach of security now admitted to be of enormous impact went undetected for some 20 years. Once again, the effort to be "all-safe" led not merely to being "half-safe" but to not being safe at all.

Ultimately, the debate over risk comes down to how best respond to dangers that cannot be fully comprehended in advance. My vote goes to the resilience that comes from passing many trials and learning from many errors so that the defects of society's limited current imagination are made up by larger amounts of global resources that can be converted into meeting the dangers that its members never thought would arise.

Safety is not a wild flower that exists fully formed in nature waiting only to be plucked whole. This flower is a product of a search among the weeds. Consider the common definition: weeds are misplaced flowers. Safety results from a process of discovery. Attempting to short-circuit this competitive, evolutionary, trial and error process by wishing the end without providing the means, is bound to be self-defeating. Safety without risk is like love without the danger of rejection; courting the one is the way to the other.